PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : H04M 17/00 — A1

(11) Numéro de publication internationale: **WO 99/49647**

(43) Date de publication internationale: 30 septembre 1999 (30.09.99)

(21) Numéro de la demande internationale: PCT/FR99/00603

(22) Date de dépôt international: 17 mars 1999 (17.03.99)

(30) Données relatives à la priorité:
98/03482 20 mars 1998 (20.03.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: BASQUIN, Bruno [FR/FR]; 132, boulevard de la Grotte Roland, F–13008 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F–13881 Gemenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: MOBILE TELEPHONE SYSTEM WITH PREPAID CARD

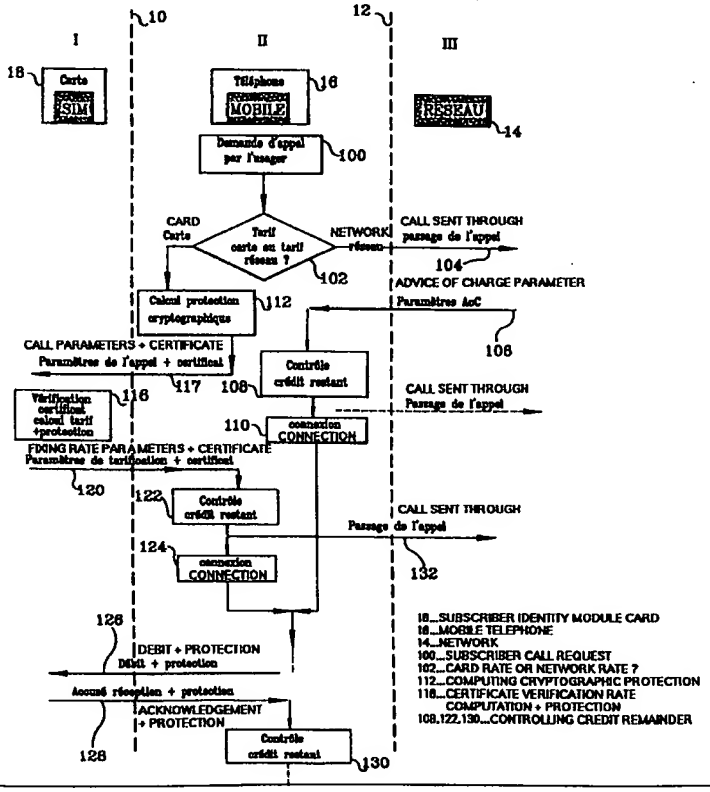
(54) Titre: SYSTEME DE TELEPHONIE MOBILE AVEC CARTE DE PREPAIEMENT

(57) Abstract

The invention concerns mobile telephones with prepaid cards, characterised in that the prepaid card (18) contains the rate fixing parameters (120) used by the mobile telephone (16) to compute the amounts to be debited (126) on the card pay units counter. The message exchanges between the mobile telephone and the card are encrypted to ensure the security of transactions, preferably by using a cryptographic certificate.

(57) Abrégé

L'invention concerne les téléphones mobiles utilisant des cartes de prépaiement. L'invention réside dans le fait que la carte à prépaiement (18) contient les paramètres de tarification (120) qui sont utilisés par le téléphone mobile (16) pour calculer les débits (126) à effectuer sur le compteur d'unités de paiement de la carte. Les échanges de messages entre le téléphone mobile et la carte sont chiffrés pour assurer la sécurité des transactions, de préférence en utilisant un certificat cryptographique.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

SYSTEME DE TELEPHONIE MOBILE AVEC CARTE DE PREPAIEMENT

L'invention concerne les téléphones mobiles qui sont utilisés avec des cartes de prépaiement.

Un réseau de téléphones mobiles, qu'il soit du type GSM ou DCS, correspondant respectivement aux acronymes anglo-saxons "Global System for Mobiles" et "Digital Cellular System", peut être représenté comme comprenant deux parties :

- une partie accessible à l'utilisateur : le téléphone mobile et la carte,
- une partie sous contrôle de l'opérateur du réseau : l'infrastructure.

Avec cette représentation, les systèmes de prépaiement peuvent se classer en trois grandes catégories selon que les fonctions de prépaiement sont réalisées.

(a) uniquement par l'infrastructure,

(b) en partie par l'infrastructure et en partie par le téléphone mobile et la carte,

(c) uniquement par le téléphone mobile et la carte.

Les systèmes des catégories (a) et (b) existent en exploitation commerciale mais présentent les inconvénients suivants :

- ils nécessitent un investissement lourd entièrement supporté par l'opérateur,
- ils nécessitent une maintenance importante d'où un coût rémanent,
- ils obligent à modifier certaines fonctions du réseau,
- ils doivent être dimensionnés en fonction du nombre d'utilisateurs, d'où une mise à jour permanente.

Pour pallier ces différents inconvénients, l'invention a pour but de réaliser un système de la catégorie (c)

dans lequel toutes les opérations de tarification des services sont réalisées par le téléphone mobile et la carte à mémoire de manière totalement autonome.

Cependant, il est à noter qu'il existe un système dans lequel l'infrastructure fournit au téléphone mobile et à la carte, un avis de coût, plus connu sous l'acronyme anglo-saxon AoC pour "Advice of Charge". Un tel système AoC présente les inconvénients suivants :

- pour chaque appel, la tarification à appliquer est envoyée par l'infrastructure du réseau, ce qui signifie que cette dernière doit être prévue à cet effet. Actuellement, peu de réseaux installés comportent cette fonction ;
- les tables de tarification sont logées dans le réseau de sorte que la tarification est figée, ce qui ne correspond pas au voeu de l'opérateur du réseau ;
- la gestion du compte d'unités du paiement se fait à travers l'interface téléphone mobile/carte par échange de commandes standards sans mesure de sécurité particulière.

Le but de l'invention est de garantir que l'utilisateur du réseau s'acquitte de manière incontournable de ses communications par le biais de sa carte prépayée.

Le principe de l'invention consiste à proposer des moyens permettant de sécuriser toutes les opérations liées à la gestion des unités de paiement, à la tarification, et au débit proprement dit, ainsi que des moyens permettant de déclencher l'authentification du mobile et/ou la carte à des instants choisis par l'opérateur.

Un autre objet de l'invention est de proposer des moyens permettant l'interopérabilité entre tous les mobiles, les cartes de prépaiement (cartes avec ou sans

table de tarification interne) ou cartes à abonnement standard.

A cet effet, le mobile comporte un mécanisme permettant de sélectionner le mode de fonctionnement approprié au type de carte ci-dessus.

Le but de l'invention est atteint par un système dans lequel :

- le téléphone mobile et la carte comportent des fonctionnalités spécifiques pour réaliser l'application de prépaiement selon l'invention ;
- l'ensemble téléphone mobile/carte détermine de manière autonome la facturation du service ;
- l'ensemble téléphone mobile/carte gère le compte de l'usager,
- le compteur d'unités de paiement est localisé dans la carte, et
- les échanges d'informations entre le téléphone mobile et la carte sont protégés contre les fraudes éventuelles.

A titre d'option, il peut être prévu un serveur connecté au réseau pour envoyer des ordres de rechargement ou de gestion des paramètres vers l'ensemble téléphone mobile/carte.

L'invention concerne un système de téléphonie mobile avec carte de prépaiement dans lequel une carte de prépaiement est associée à un téléphone mobile connecté à un réseau téléphonique, caractérisé en ce que :

- la carte de prépaiement comprend au moins un microprocesseur pour effectuer des calculs cryptographiques en vue de chiffrer et/ou déchiffrer des messages numériques et un compteur d'unités de paiement, contenant la valeur prépayée,
- le téléphone mobile comprend au moins un microprocesseur pour effectuer des calculs de débit

en fonction des caractéristiques de l'appel téléphonique et de l'usager du téléphone ainsi que des calculs cryptographiques en vue de chiffrer et/ou déchiffrer des messages numériques, un dispositif d'enregistrement et de lecture de la carte de prépaiement pour échanger lesdits messages numériques chiffrés ou non avec ladite carte de prépaiement et,

- chaque message numérique enregistré ou lu dans la carte de prépaiement est chiffré et/ou déchiffré à l'aide d'un certificat cryptographique contenu dans le message numérique.

Dans un exemple préféré de réalisation du système, la carte de prépaiement comprend, en outre, une mémoire pour enregistrer les paramètres de la tarification appliquée à l'usager.

Pour enregistrer le certificat cryptographique de chaque message numérique chiffré, le téléphone mobile et la carte de prépaiement comprennent chacun, en outre, une mémoire à cet effet.

Pour augmenter la sécurité du chiffrement et du déchiffrement, le téléphone mobile et la carte de prépaiement comprennent chacun, en outre, un compteur qui est chargé avec un code aléatoire fourni par le réseau et qui s'incrémente d'un même nombre d'unités à des instants déterminés.

L'invention concerne également un procédé pour mettre en oeuvre le système de téléphonie avec carte de prépaiement, caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) mettre sous tension le téléphone mobile,

(b) reconnaître la présence ou l'absence d'une carte prépayée connectée au téléphone mobile, et

- aller à l'étape (c) en cas d'absence de la carte ou,

- aller aux étapes (d) et suivantes en cas de présence de la carte,

(c) opérer le téléphone mobile de manière classique en cas d'absence de carte prépayée,

(d) lire dans la carte prépayée le numéro d'identification international de l'usager de la carte de prépaiement,

(e) inscrire, dans le téléphone mobile, l'usager de la carte de prépaiement en tant qu'utilisateur du réseau sous le numéro d'identification international,

(f) authentifier, à la demande du réseau, le téléphone mobile en tant qu'utilisateur autorisé de la carte de prépaiement,

(g) lire dans la carte de prépaiement les paramètres de la tarification de l'appel de l'usager ainsi que le crédit de paiement restant sur le compteur d'unités de paiement,

(h) passer l'appel si le crédit de paiement restant est suffisant, et

(i) calculer dans le téléphone mobile, au fur et à mesure de la durée de la liaison téléphonique, le nombre d'unités de paiement à débiter,

(j) débiter le compteur d'unités de paiement d'un nombre d'unités correspondant à la liaison téléphonique en cours.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description suivante, ladite description étant faite en relation avec les dessins joints dans lesquels :

- la figure 1 est un diagramme montrant les opérations à effectuer en vue d'obtenir la sécurité des échanges ou transactions entre le téléphone mobile et la carte,

- la figure 2 est un diagramme montrant les opérations à effectuer en vue de reconnaître et activer une carte de prépaiement avec un téléphone mobile habilité,
- la figure 3 est un diagramme montrant les opérations à effectuer en vue d'authentifier périodiquement le téléphone mobile par la carte, et
- la figure 4 est un diagramme montrant les opérations à effectuer en vue de choisir la tarification et de débiter la carte.

Chaque figure a été divisée en trois parties verticales I, II et III séparées par deux traits discontinus 10 et 12 pour indiquer les trois éléments du système, savoir un réseau ou infrastructure 14, un téléphone mobile 16 et une carte à prépaiement 18 qui est souvent désignée sous l'appellation carte SIM, SIM étant l'acronyme anglo-saxon pour Subscriber Identification Module, c'est-à-dire le module d'identification de l'usager ou abonné. Les opérations indiquées dans chaque partie verticale I, II ou III sont réalisées par l'élément correspondant et les échanges d'informations entre les éléments sont matérialisés par des flèches horizontales reliant les parties concernées par l'échange.

Afin d'assurer la sécurité des échanges d'informations contre les fraudes, l'invention prévoit que ces échanges soient effectués en mettant en oeuvre des procédés cryptographiques selon le diagramme de la figure 1.

Sur cette figure 1, le téléphone mobile 16 élabore une commande 20 qui, si elle est critique pour la sécurité, est chiffrée par une opération 22 de calculs cryptographiques.

Il s'agit d'une commande ou d'un message critique qui a un impact sur la gestion des unités de paiement,

notamment facturation, lecture de la tarification, décompte des unités de paiement, mais également sur l'authentification réciproque entre la carte et le mobile. Certaines commandes qui ne sont pas critiques du point de vue de la sécurité ne sont pas chiffrées.

La commande chiffrée ou non est transmise à la carte 18. La commande chiffrée peut contenir un certificat cryptographique qui permet sa certification par la carte 18. Selon une variante préférée qui est représentée sur la figure 1, la commande est transmise sans chiffrement (24) mais, en parallèle, un certificat cryptographique est transmis (26) à la carte et est enregistré par le téléphone dans un fichier de la carte appelé "boîte à lettres". L'avantage de procéder ainsi est d'utiliser des messages ou commandes au format standard. On utilise ce certificat pour effectuer des calculs cryptographiques de manière à vérifier qu'il s'agit d'une commande chiffrée (28) prévue par le système.

Si la vérification ou certification n'est pas valide (30), la carte transmet au téléphone mobile un signal d'erreur (32). En cas de validation de la certification, la commande est exécutée (34). L'exécution de la commande donne lieu à l'élaboration de la réponse de la carte (opération 36), réponse qui est de préférence chiffrée (opération 38), surtout s'il s'agit de réponses à des commandes critiques telles que visées ci-dessus avec enregistrement d'un certificat cryptographique dans la boîte à lettres (opération 40). La réponse est transmise au téléphone mobile (opération 42) tandis que le certificat cryptographique est lu par le téléphone mobile dans la boîte à lettres (opération 44) pour servir au traitement cryptographique (vérification) (opération 46) dans le téléphone mobile.

Il est à remarquer que l'accès à la boîte à lettres est effectué à l'aide de commandes classiques sans sécurité. Comme décrit ci-dessus, la sécurisation des échanges bilatéraux téléphone mobile/carte repose sur un calcul cryptographique effectué par la partie qui transmet et vérifié par la partie qui reçoit, ce calcul étant effectué à chaque transmission de donnée entre le téléphone mobile et la carte.

Pour éviter que le résultat du calcul cryptographique soit identique pour deux commandes identiques dans leur contenu, l'invention prévoit un mécanisme anti-rejeu qui consiste à introduire dans le calcul cryptographique une donnée variable arbitraire qui a une très faible probabilité de reprendre deux fois la même valeur.

Cette donnée variable peut être obtenue à l'aide d'un compteur dans le téléphone mobile et la carte, compteur qui est actualisé indépendamment par chaque partie à l'échange et qui s'incrémente d'une unité à chaque calcul cryptographique. Mais une telle valeur de compteur doit être conservée d'une session à l'autre, ce qui implique qu'un téléphone mobile à prépaiement donné ne fonctionne qu'avec une carte à prépaiement donnée et présente l'inconvénient d'être limitatif.

Pour pallier cet inconvénient, l'invention utilise un nombre aléatoire, appelé "random". De préférence, pour des raisons de facilité de mise en oeuvre, on utilise le "random" qui se trouve dans la demande d'authentification émise de manière classique par le réseau. Ainsi, à chaque demande d'authentification par le réseau, le téléphone mobile et la carte enregistrent chacun la valeur du "random" comme nouvelle valeur initiale du compteur et à chaque nouvelle commande ou réponse certifiée qui doit être échangée entre le

téléphone mobile et la carte, chaque partie utilisera la valeur de son compteur telle quelle puis l'incrémentera d'un même nombre fixe d'unités à chaque échange de donnée ou de commande.

Pour qu'un téléphone mobile sans prépaiement ne soit pas capable de générer une demande d'inscription sur le réseau avec une carte de prépaiement, l'invention prévoit de désactiver certaines fonctions de la carte (opération 50, figure 2) après sa mise sous tension (opération 52) par le téléphone mobile et à l'activer seulement par un téléphone mobile habilité.

Pour que le téléphone mobile puisse fonctionner à la fois avec des cartes à prépaiement et des cartes d'abonnement normales, il est nécessaire de mettre en place une procédure de reconnaissance mutuelle. A cet effet, toute session débute par la reconnaissance de la carte par le téléphone mobile (opération 54) par inspection des données de configuration de la carte sans sécurité particulière car une carte qui prétendrait être ce qu'elle n'est pas serait rejetée lors des procédures ultérieures. Au cas où cette reconnaissance échoue (opération 58), le système fonctionne de manière classique sans prépaiement (opération 60). Si la carte est reconnue comme étant à prépaiement, le téléphone mobile transmet à la carte une commande de lecture (opération 62) du code international de l'abonné plus connu sous l'acronyme anglo-saxon IMSI pour International Mobile Subscriber Identification. Cette commande de lecture du code IMSI est effectuée avec certification, certification qui est validée on non par la carte (opération 64).

Si la commande de lecture du code IMSI n'est pas validée, la carte transmet au téléphone mobile un signal d'erreur (opération 66). Dans le cas contraire,

la carte est entièrement activée et se met en position d'attente (opération 72) ; elle transmet son code IMSI (opération 70) au téléphone mobile qui inscrit l'abonné au réseau et attend une demande d'authentification (opération 72).

Cette lecture certifiée du code IMSI permet d'éviter qu'un téléphone mobile fonctionnant sans prépaiement puisse activer une carte à prépaiement et générer une requête d'inscription sur le réseau. La carte de prépaiement ne transmet son code IMSI que si la commande de lecture est correctement certifiée.

Il faut ensuite vérifier que le téléphone mobile est habilité à exploiter une carte de prépaiement pour garantir que la gestion des unités de paiement est correctement effectuée. A cet effet, l'invention prévoit que, à la demande périodique du réseau, le téléphone mobile prouve de préférence répétitivement à la carte et vice-versa qu'il est habilité à opérer une carte à prépaiement. Avantageusement, cette vérification de l'authenticité du mobile et/ou de la carte est déclenchée extérieurement et de manière non prévisible par l'utilisateur par une procédure existante au niveau du réseau. En particulier, la demande d'authentification de la carte par le réseau convient en tant que procédure externe qui force une interaction entre le mobile et la carte.

Ainsi (figure 3), le réseau transmet au téléphone mobile une demande d'authentification (opération 80) qui la transmet à la carte (opération 84) après calcul cryptographique (opération 82) sous une forme chiffrée avec un certificat cryptographique comme décrit ci-dessus.

La carte effectue un calcul cryptographique pour authentifier la demande (opération 86).

Si la certification n'est pas validée (opération 88), la carte transmet un signal d'erreur (opération 90) au téléphone mobile qui le retransmet (opération 92) au réseau. Ce dernier rejette alors le téléphone mobile (opération 94).

Si la certification est validée, la carte transmet sa réponse au téléphone mobile (opération 96) qui la retransmet au réseau (opération 98).

Selon l'invention, les paramètres de tarification sont calculés par la carte en fonction des caractéristiques de l'appel telles que le numéro demandé, l'heure, la zone de localisation, etc ... . Ces calculs sont effectués à partir de tables de tarification enregistrées dans des fichiers internes à la carte. Le format des paramètres transmis par la carte au téléphone mobile et la manière de les traiter par ce dernier peuvent être du type AoC (Advance of Charge) et sont décrits dans la norme d'exploitation du système GSM.

Ainsi, en utilisant les normes GSM de tarification AoC dans le téléphone mobile, il est possible de traiter aussi bien des tarifications fournies par la carte que des tarifications fournies par le réseau. Le choix entre l'une ou l'autre tarification est réalisé notamment par une détection sécurisée de la présence des fichiers de tarification dans la carte.

Les paramètres de tarification sont traités par le téléphone mobile pour déterminer la manière de débiter le compteur d'unités de paiement au cours de l'appel. Par exemple, un débit forfaitaire à la prise de ligne, puis un débit d'unités de paiement en fonction du temps. Dans ce cas, la périodicité avec laquelle le mobile vient débiter le compteur dans la carte est définie par les paramètres de tarification.

Le crédit restant dans le compteur d'unités de paiement de la carte est contrôlé par le téléphone mobile au moment d'accorder le service à l'usager, puis à chaque opération de débit durant l'appel.

Les décisions prises par le téléphone mobile en fonction de l'état du compteur sont de préférence conformes à ce qui est décrit pour l'AoC dans la norme GSM.

Les opérations qui sont effectuées pour le choix de la tarification et le débit d'unités dans la carte à prépaiement seront décrites en relation avec la figure 4.

A la demande d'appel de l'usager (opération 100), le téléphone mobile transmet à la carte les paramètres de l'appel (opération 114) de préférence sous forme sécurisée par un calcul cryptographique (opération 112) avec un certificat cryptographique. La carte vérifie la certification (opération 116) et si cette vérification est valide, transmet de préférence sous forme sécurisée (opération 120) les paramètres de tarification ainsi que le crédit restant au téléphone mobile.

Le téléphone mobile contrôle le crédit restant (opération 122) et autorise ou non le passage de l'appel vers le réseau (opération 132). Lorsque la connexion est établie (opération 124), le téléphone mobile transmet sous forme sécurisée à la carte le débit en unités de paiement au fur et à mesure de la durée de la liaison téléphonique (opération 126). La carte répond par un accusé de réception, également sécurisé, (opération 128), avec un montant de crédit restant qui est contrôlé par le téléphone mobile (opération 130).

Dans le cas où la carte ne contient pas de paramètres de tarification, le téléphone mobile en déduit

(opération 102) que le tarif est celui du réseau et permet le passage de l'appel (opération 104). Le réseau répond en transmettant au téléphone mobile les paramètres de l'AoC (opération 106) avec lesquels ce dernier calcule le coût à débiter. Après contrôle du crédit restant dans la carte (opération 108), le téléphone mobile autorise ou non la connexion (opération 110) et effectue avec la carte les opérations 126 et 128 pour débiter la carte.

La description de la figure 4 montre que toutes les commandes de débit et les accusés de réception sont sécurisés à l'aide du procédé de sécurisation décrit en relation avec la figure 1. Par ce procédé, on assure que le débit effectué dans la carte est authentique, intègre et correctement réalisé dans une carte à prépaiement valide.

Comme indiqué ci-dessus, l'accusé de réception pourra contenir la valeur actualisée du compteur d'unités de paiement, évitant ainsi au mobile de générer une commande séparée pour connaître la valeur restant dans le compteur.

En début de session, le téléphone mobile est capable de lire de manière sécurisée la valeur du compteur dans la carte en transmettant une commande de débit nul.

La description qui vient d'être faite en relation avec les figures 1 et 4 permet de définir les différentes étapes d'un procédé pour mettre en oeuvre le système de téléphonie mobile, ces étapes consistant à :

(a) mettre sous tension le téléphone mobile 16,

(b) reconnaître la présence ou l'absence d'une carte prépayée 18 connectée au téléphone mobile, et

- aller à l'étape (c) en cas d'absence de la carte de prépaiement ou,

- aller aux étapes (d) et suivantes en cas de présence de la carte de prépaiement,

(c) opérer le téléphone mobile de manière classique en cas d'absence de carte prépayée,

(d) lire dans la carte prépayée le numéro d'identification international de l'usager de la carte de prépaiement,

(e) inscrire, dans le téléphone mobile, l'usager de la carte de prépaiement en tant qu'utilisateur du réseau sous le numéro d'identification international,

(f) provoquer une procédure d'authentification réciproque entre le mobile et la carte de prépaiement,

(g) lire dans la carte de prépaiement les paramètres de la tarification de l'appel de l'abonné ainsi que le crédit de paiement restant sur le compteur d'unités de paiement,

(h) passer l'appel si le crédit de paiement restant est suffisant, et

(i) calculer dans le téléphone mobile, au fur et à mesure de la durée de la liaison téléphonique, le nombre d'unités de paiement à débiter,

(j) débiter le compteur d'unités de paiement d'un nombre d'unités correspondant à la liaison téléphonique en cours.

L'étape (f) est déclenchée à la demande du réseau, lors d'une demande d'inscription au réseau (connexion) sous le numéro d'identification lu dans la carte et est de préférence répétée de temps à autre au cours d'une session de connexion pour renouveler l'authentification et éviter ainsi un éventuel remplacement du module et/ou de la carte pendant la session.

L'étape (j) est également répétée pour débiter le compteur d'unités de paiement de manière à vérifier le crédit restant.

Afin d'empêcher les fraudes, on ajoute au moins l'une, voire toutes les étapes (d), (e), (f), (g) et (j) qui sont réalisées sous une forme sécurisée selon les principes décrits en relation avec la figure 1 :

(A) effectuer des calculs cryptographiques sur le message numérique à transmettre à l'aide d'une clé cryptographique et/ou d'un code (nombre) contenu dans un compteur de l'émetteur du message,

(B) transmettre le message numérique chiffré et le certificat cryptographique au récepteur du message,

(C) effectuer des calculs cryptographiques sur le message numérique chiffré à l'aide du certificat cryptographique et d'un code contenu dans un compteur du récepteur,

Pour améliorer cette sécurité, le compteur de l'émetteur du message numérique et celui du récepteur du message numérique sont chargés par un même code aléatoire, appelé "random", fourni par le réseau.

L'étape (f) d'authentification du téléphone mobile associé à la carte de prépaiement comprend les étapes intermédiaires suivantes consistant à :

(f_1) réaliser par le réseau une demande d'authentification au téléphone mobile,

(f_2) chiffrer, dans le téléphone mobile, cette demande d'authentification,

(f_3) transmettre à la carte de prépaiement un message numérique contenant cette demande d'authentification cryptée,

(f_4) déchiffrer, dans la carte de prépaiement, le message numérique transmis par le téléphone mobile,

(f_5) déterminer, dans la carte de prépaiement, si la demande d'authentification du réseau transmise par le téléphone mobile est valide ou non, et

- aller aux étapes (f_6) et (f_7) en cas d'absence de validation,
- aller aux étapes (f_8) et (f_9) en cas de validation,

(f_6) transmettre au réseau un signal d'erreur par l'intermédiaire du téléphone mobile, et

(f_7) rejeter le téléphone mobile comme utilisateur du réseau avec la carte de prépaiement associée,

(f_8) transmettre au réseau un signal de validation par l'intermédiaire du téléphone mobile, et

(f_9) reconnaître le téléphone mobile comme utilisateur du réseau avec la carte de prépaiement associée.

La description qui vient d'être faite de l'invention montre qu'elle met en jeu uniquement les téléphones mobiles et les cartes à prépaiement. Il en résulte :

- un investissement minimal pour l'opérateur,
- peu de besoins en installation,
- une croissance du parc limitée seulement par la capacité du réseau,
- l'absence de surcoût.

Par ailleurs, tous les échanges entre le téléphone mobile et la carte et notamment ceux relatifs à la tarification sont sécurisés de sorte que la possibilité de fraudes est liée à la résistance aux attaques de l'algorithme cryptographique et non plus à la faculté de filtrer les commandes au niveau de l'interface téléphone mobile/carte.

Enfin, la tarification est calculée par la carte à l'aide de tables internes contenues dans la carte de sorte que les tables de tarification peuvent être modifiées par personnalisation ou par

téléadministration. Il en résulte qu'un opérateur peut mettre en oeuvre ses propres stratégies commerciales de tarification en intervenant au niveau des cartes.

REVENDICATIONS

1. Système de téléphonie mobile avec carte de prépaiement (18) comportant un numéro d'identification international de l'usager de ladite carte, un compteur d'unités de paiement contenant une valeur prépayée, dans lequel une carte de prépaiement (18) est associée à un téléphone mobile (16) connecté à un réseau téléphonique (14), caractérisé en ce que :

- la carte de prépaiement (18) comprend au moins un microprocesseur pour effectuer des calculs cryptographiques de messages critiques,
- le téléphone mobile (16) comprend au moins un microprocesseur pour effectuer des calculs de débit en fonction de tarifications téléphoniques (AoC) ainsi que des calculs cryptographiques de messages critiques, un dispositif d'enregistrement et de lecture de la carte de prépaiement pour échanger lesdits messages numériques chiffrés ou non avec ladite carte de prépaiement (18) et,
- chacun desdits messages numériques critiques étant chiffrés ou associés à un certificat cryptographique transmis séparément en vue de sécuriser les échanges de messages élaborés entre le mobile et la carte.

2. Système selon la revendication 1, caractérisé en ce que la carte de prépaiement comprend, en outre, une mémoire pour enregistrer les paramètres de la tarification appliquée à l'usager, lesdits paramètres étant lus dans la carte par le téléphone mobile.

3. Système selon la revendication 1, caractérisé en ce que les paramètres de la tarification appliquée à l'usager sont fournis par le réseau (AoC).

4. système selon la revendication 1, 2 ou 3, caractérisé en ce que la carte de prépaiement (18) et le téléphone mobile (16) comprennent chacun, en outre, une mémoire pour enregistrer ledit certificat cryptographique.

5. Système selon la revendication 1, 2, 3 ou 4, caractérisé en ce que la carte de prépaiement (18) et le téléphone mobile (16) comprennent chacun, en outre, un compteur prévu pour augmenter d'un même nombre d'unités à chaque calcul cryptographique et apte à être initialisé par un nombre aléatoire fourni par le réseau (14).

6. Procédé pour mettre en ouvre le système de téléphonie avec carte de prépaiement selon l'une des revendications précédentes, caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) mettre sous tension le téléphone mobile (16),

(b) reconnaître la présence ou l'absence d'une carte prépayée (18) connectée au téléphone mobile, et

- aller à l'étape (c) en cas d'absence de la carte ou,

- aller aux étapes (d) et suivantes en cas de présence de la carte,

(c) opérer le téléphone mobile de manière classique en cas d'absence de carte prépayée,

(d) lire de manière sécurisée dans la carte prépayée le numéro d'identification international de l'usager de la carte de prépaiement,

(e) inscrire, dans le téléphone mobile, l'usager de la carte de prépaiement en tant qu'utilisateur du réseau sous le numéro d'identification international,

(f) provoquer une procédure d'authentification réciproque entre le mobile et la carte de

prépaiement pour demander une inscription au réseau sous le numéro d'identification lu dans la carte,

(g) lire dans la carte de prépaiement les paramètres de la tarification de l'appel de l'abonné ainsi que le crédit de paiement restant sur le compteur d'unités de paiement,

(h) passer l'appel si le crédit de paiement restant est suffisant, et

(i) calculer dans le téléphone mobile, au fur et à mesure de la durée de la liaison téléphonique, le nombre d'unités de paiement à débiter,

(j) débiter le compteur d'unités de paiement d'un nombre d'unités correspondant à la liaison téléphonique en cours.

7. Procédé selon la revendication 6, caractérisé en ce que les étapes (f) et (j) sont répétées de temps à autre au cours d'une liaison téléphonique.

8. Procédé selon la revendication 6 ou 7, caractérisé en ce que les étapes (d), (e), (f), (g) et (j) sont réalisées sous forme sécurisée.

9. Procédé selon la revendication 8, caractérisé en ce que les opérations pour sécuriser les étapes (d), (e), (f), (g) et (j), consistent à :

(A) effectuer des calculs cryptographiques sur le message numérique à transmettre à l'aide d'une clé cryptographique et/ou d'un code (nombre) contenu dans un compteur de l'émetteur du message,

(B) transmettre le message numérique chiffré et le certificat cryptographique au récepteur du message,

(C) effectuer des calculs cryptographiques sur le message numérique chiffré à l'aide du certificat

cryptographique et d'un code contenu dans un compteur du récepteur,

le compteur de l'émetteur et le compteur du récepteur étant préalablement positionnés à une même valeur de code et étant avancés d'un même nombre d'unités à des instants déterminés.

10. Procédé selon la revendication 9, caractérisé en ce que le code contenu dans le compteur de l'émetteur du message et dans le compteur du récepteur du message est un code aléatoire fourni par le réseau.

11. Procédé selon l'une quelconque des revendications 9 ou 10, caractérisé en ce que l'étape (f) consiste dans les étapes intermédiaires suivantes consistant à :

(f_1) réaliser par le réseau une demande d'authentification au téléphone mobile,

(f_2) crypter, dans le téléphone mobile, cette demande d'authentification,

(f_3) transmettre à la carte de prépaiement un message numérique contenant cette demande d'authentification cryptée,

(f_4) décrypter, dans la carte de prépaiement, le message numérique transmis par le téléphone mobile,

(f_5) déterminer, dans la carte de prépaiement, si la demande d'authentification du réseau transmise par le téléphone mobile est valide ou non, et

- aller aux étapes (f_6) et (f_7) en cas d'absence de validation,
- aller aux étapes (f_8) en cas de validation,

(f_6) transmettre au réseau un signal d'erreur par l'intermédiaire du téléphone mobile, et

(f_7) rejeter le téléphone mobile comme utilisateur du réseau avec la carte de prépaiement associée,

(f_8) transmettre au réseau un signal de validation par l'intermédiaire du téléphone mobile, et

(f_9) reconnaître le téléphone mobile comme utilisateur du réseau avec la carte de prépaiement associée.

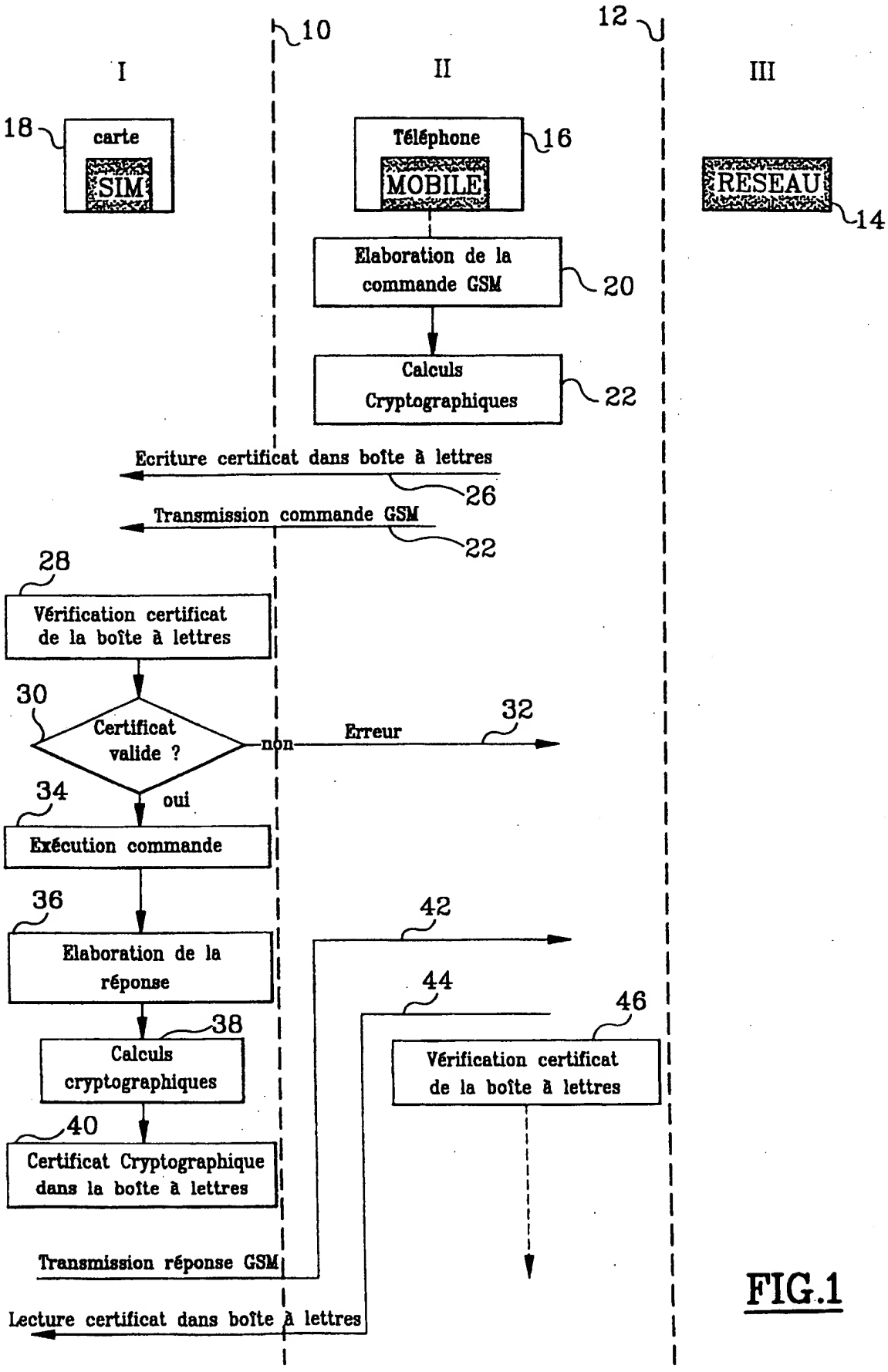

10
12
I
II
III
18
carte
SIM
Téléphone
MOBILE
16
RESEAU
14
Elaboration de la commande GSM
20
Calculs Cryptographiques
22
Ecriture certificat dans boîte à lettres
26
Transmission commande GSM
22
28
Vérification certificat de la boîte à lettres
30
Certificat valide ?
non
Erreur
32
oui
34
Exécution commande
36
Elaboration de la réponse
42
44
46
38
Calculs cryptographiques
Vérification certificat de la boîte à lettres
40
Certificat Cryptographique dans la boîte à lettres
Transmission réponse GSM
Lecture certificat dans boîte à lettres

FIG.1

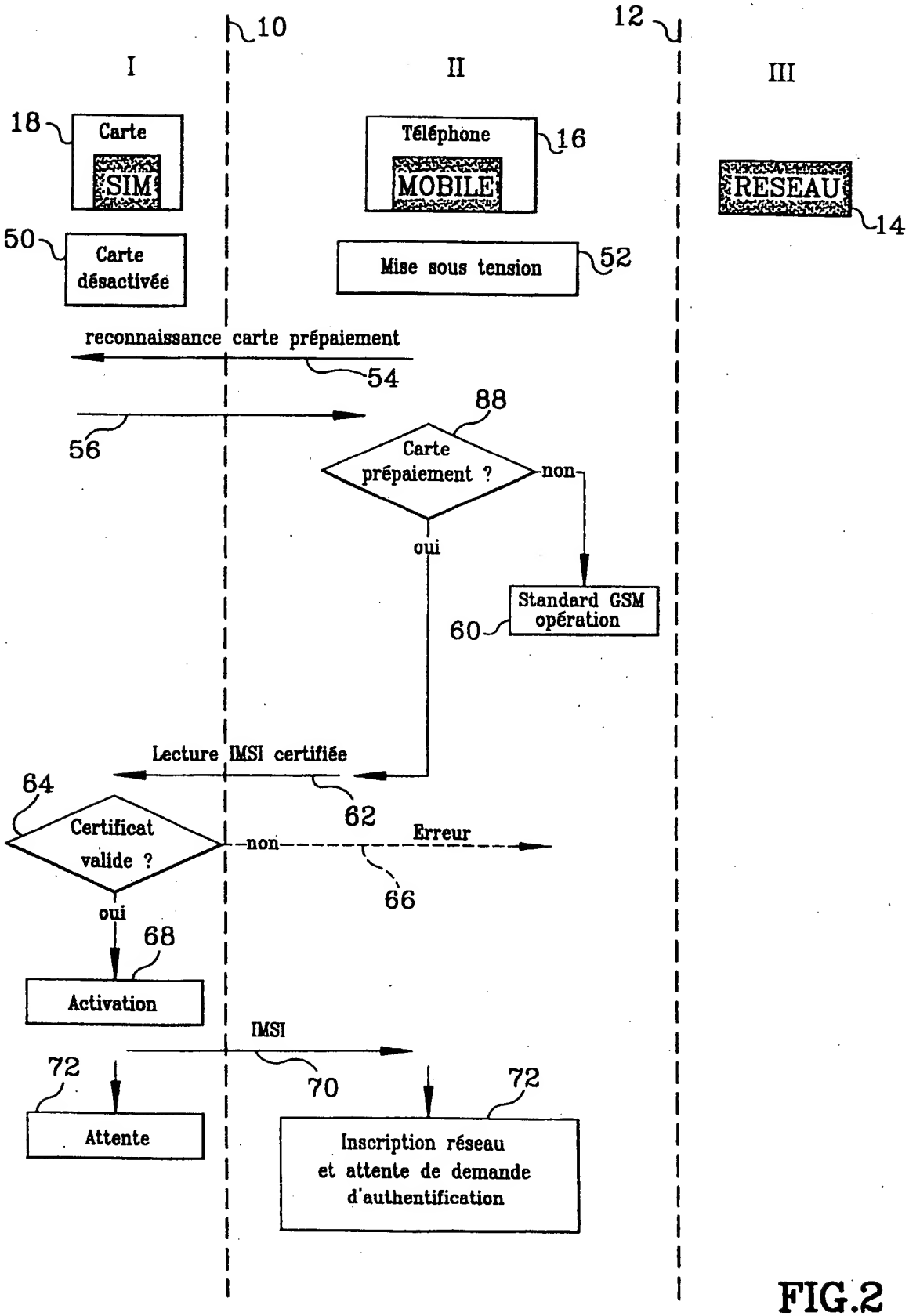

10
12
I
II
III
18
Carte
SIM
Téléphone
MOBILE
16
RESEAU
14
50
Carte désactivée
Mise sous tension
52
reconnaissance carte prépaiement
54
56
88
Carte prépaiement ?
non
oui
Standard GSM opération
60
Lecture IMSI certifiée
62
64
Certificat valide ?
non
Erreur
66
oui
68
Activation
IMSI
70
72
72
Attente
Inscription réseau et attente de demande d'authentification

FIG.2

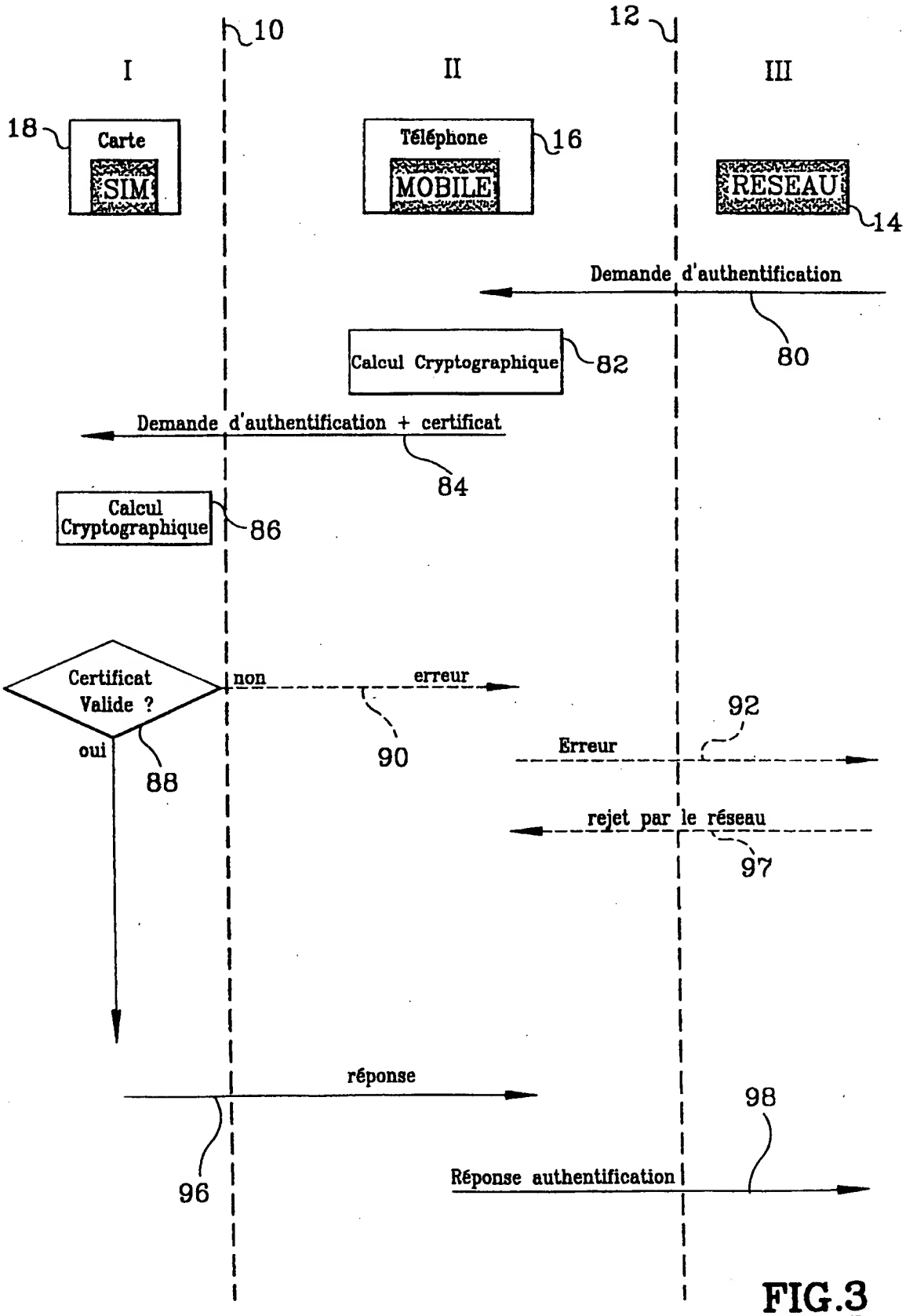

10
12
I
II
III
18
Carte
SIM
Téléphone
MOBILE
16
RESEAU
14
Demande d'authentification
80
Calcul Cryptographique
82
Demande d'authentification + certificat
84
Calcul Cryptographique
86
Certificat Valide ?
non
erreur
90
92
Erreur
oui
88
rejet par le réseau
97
réponse
96
98
Réponse authentification

FIG.3

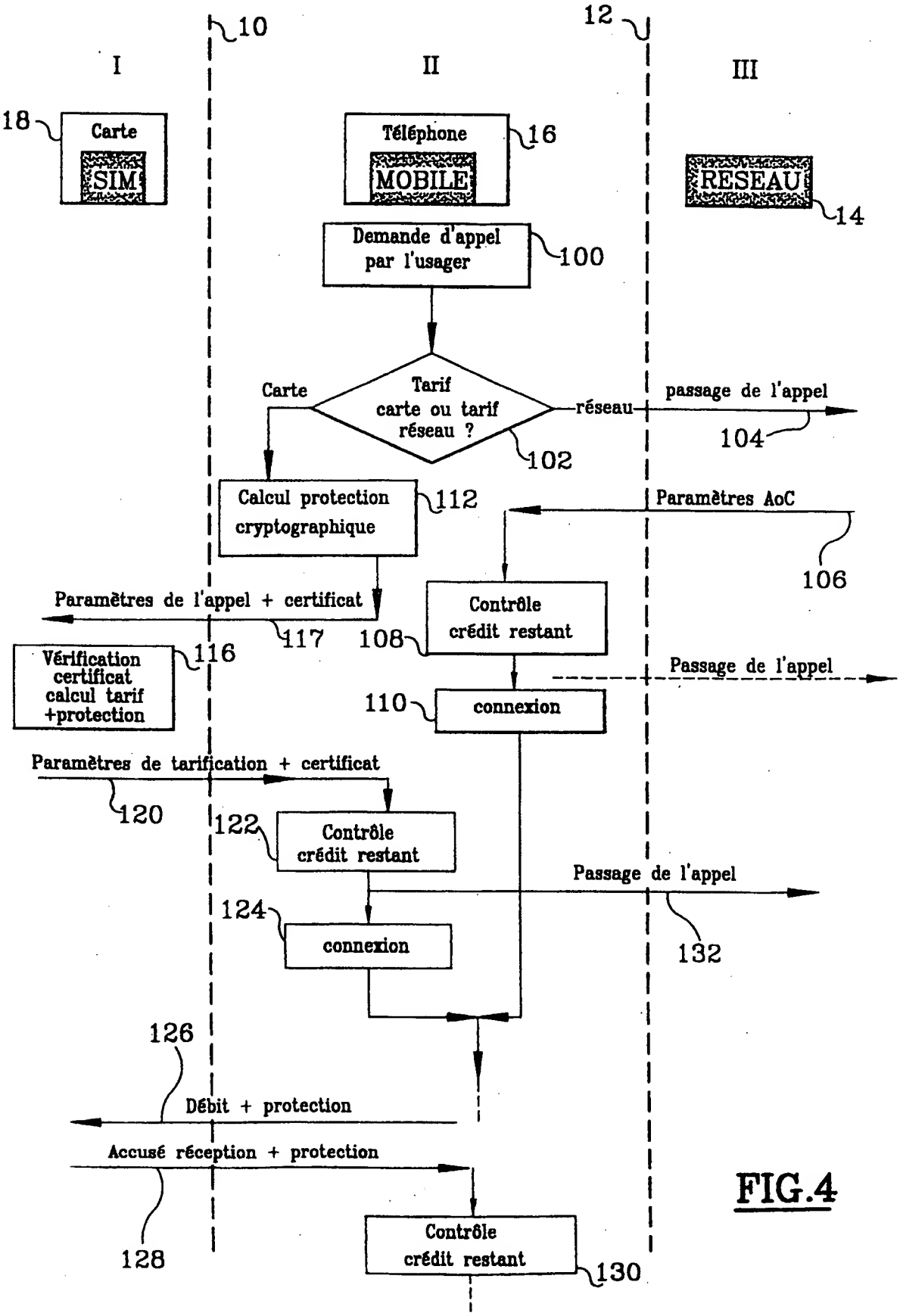

10
12
I
II
III
18
Carte
SIM
Téléphone
16
MOBILE
RESEAU
14
Demande d'appel par l'usager
100
Carte
Tarif carte ou tarif réseau ?
réseau
passage de l'appel
102
104
Calcul protection cryptographique
112
Paramètres AoC
106
Paramètres de l'appel + certificat
117
Contrôle crédit restant
108
Vérification certificat calcul tarif +protection
116
Passage de l'appel
110
connexion
Paramètres de tarification + certificat
120
122
Contrôle crédit restant
Passage de l'appel
124
connexion
132
126
Débit + protection
Accusé réception + protection
128
Contrôle crédit restant
130

FIG.4

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/FR 99/00603

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 40616 A (GEMPLUS CARD INT) 30 October 1997 see the whole document	1-3
A	US 4 640 986 A (MAKINO MASAYUKI ET AL) 3 February 1987 see column 2, line 30 - line 45	1-11
A	EP 0 626 664 A (GEMPLUS CARD INT) 30 November 1994 see column 1, line 54 - column 3, line 51	1-11
A	EP 0 734 144 A (SIEMENS AG) 25 September 1996 see column 4, line 13 - line 33	1-11

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 July 1999	14/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Montalbano, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/FR 99/00603

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 48221 A (QUALCOMM INC) 18 December 1997 see abstract -----	1-11

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

Int tional Application No
PCT/FR 99/00603

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9740616 A	30-10-1997	AU 2401397 A	12-11-1997
		CA 2252526 A	30-10-1997
		EP 0894397 A	03-02-1999
US 4640986 A	03-02-1987	JP 60062741 A	10-04-1985
		JP 1614024 C	15-08-1991
		JP 2026897 B	13-06-1990
		JP 60062744 A	10-04-1985
		AU 577732 B	29-09-1988
		AU 3304784 A	21-03-1985
		CA 1227249 A	22-09-1987
		DE 3484913 A	19-09-1991
		EP 0135196 A	27-03-1985
EP 0626664 A	30-11-1994	FR 2704704 A	04-11-1994
		DE 69400549 D	24-10-1996
		DE 69400549 T	30-01-1997
		ES 2092867 T	01-12-1996
		JP 7073281 A	17-03-1995
		SG 48143 A	17-04-1998
		US 5687398 A	11-11-1997
		US 5896507 A	20-04-1999
EP 0734144 A	25-09-1996	NONE	
WO 9748221 A	18-12-1997	AU 3486997 A	07-01-1998
		CA 2258027 A	18-12-1997
		EP 0906688 A	07-04-1999
		NO 985813 A	02-02-1999

RAPPORT DE RECHERCHE INTERNATIONALE

De de internationale No
PCT/FR 99/00603

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04M17/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04M

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 97 40616 A (GEMPLUS CARD INT) 30 octobre 1997 voir le document en entier ---	1-3
A	US 4 640 986 A (MAKINO MASAYUKI ET AL) 3 février 1987 voir colonne 2, ligne 30 - ligne 45 ---	1-11
A	EP 0 626 664 A (GEMPLUS CARD INT) 30 novembre 1994 voir colonne 1, ligne 54 - colonne 3, ligne 51 ---	1-11
A	EP 0 734 144 A (SIEMENS AG) 25 septembre 1996 voir colonne 4, ligne 13 - ligne 33 --- -/--	1-11

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 juillet 1999	14/07/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Montalbano, F

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 99/00603

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 97 48221 A (QUALCOMM INC) 18 décembre 1997 voir abrégé	1-11

1

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 99/00603

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9740616 A	30-10-1997	AU 2401397 A	12-11-1997
		CA 2252526 A	30-10-1997
		EP 0894397 A	03-02-1999
US 4640986 A	03-02-1987	JP 60062741 A	10-04-1985
		JP 1614024 C	15-08-1991
		JP 2026897 B	13-06-1990
		JP 60062744 A	10-04-1985
		AU 577732 B	29-09-1988
		AU 3304784 A	21-03-1985
		CA 1227249 A	22-09-1987
		DE 3484913 A	19-09-1991
		EP 0135196 A	27-03-1985
EP 0626664 A	30-11-1994	FR 2704704 A	04-11-1994
		DE 69400549 D	24-10-1996
		DE 69400549 T	30-01-1997
		ES 2092867 T	01-12-1996
		JP 7073281 A	17-03-1995
		SG 48143 A	17-04-1998
		US 5687398 A	11-11-1997
		US 5896507 A	20-04-1999
EP 0734144 A	25-09-1996	AUCUN	
WO 9748221 A	18-12-1997	AU 3486997 A	07-01-1998
		CA 2258027 A	18-12-1997
		EP 0906688 A	07-04-1999
		NO 985813 A	02-02-1999